Bridging the Planning Gap: Incorporating Cyberspace Into Operational Planning

May 4, 2015 | Colonel Martha S. H. VanDriel

Cyberspace operations have a far-reaching, permanent impact on military operations. At the conceptual level, the U.S. Department of Defense (DoD) now recognizes five warfighting domains: land, maritime, air, space, and cyber.[1] While there are examples of how cyberspace support to military operations have advanced over the past decade, one gap has not been addressed in detail—operational planning.

It is clear that in U.S. military operations, the land, maritime, air, and space domains rely **heavily** on cyberspace. Therefore, cyberspace operations must be viewed in the context of all domains and be included as part of the overall operational scheme of maneuver. For if a commander postures his or her command to fight an adversary in the first four domains but ignores cyberspace, not only will that commander have ceded the cyberspace domain to the adversary, but the adversary can then proceed to undermine that commander's effectiveness in the other four domains.

Despite this critical requirement, incorporating cyberspace operations into operational-level planning at the Army Service Component Command (ASCC), Joint Task Force (JTF), and Combatant Command (CCMD) levels has proven much more difficult than anticipated. For this reason, Joint and Army senior leaders have identified operational-level cyberspace planners to be a critical shortage.[2] However, although a number of operational-level planners have been sent to cyberspace training courses and a number of cyberspace experts have been sent to operational-

level headquarters to support planning, relatively little progress has been made overall. This is because not just one, but several major systemic obstacles hinder the incorporation of cyberspace into operational planning.

To illustrate, when a cyberspace subject matter expert (SME) arrives at an operational-level headquarters to support planning, some version of the following conversation often ensues:

G5 lead planner: Glad you're here! What can you do to help us?

Cyber SME: Well, I can't tell you what I can do; the classification is too high and it would take me too long to explain anyway. What effects do you want?

G5 lead planner: How can I tell you what effects I want if I don't even know what you can do? We're going through MDMP [the Military Decisionmaking Process] now; can't you tell us what you can do as we go through the steps?

Cyber SME: No, I need you to tell me what effects you want.

G5 lead planner: Um, okay . . . can you isolate this? [points to part of a friendly Course of Action (COA)]

Cyber SME: No…

G5 lead planner: Can you attack that? [points to another part of a friendly COA]

Cyber SME: No…

G5 lead planner: Then can you do this? [points to still another part of a friendly COA]

Cyber SME: No…

G5 lead planner: (Frustrated) Then what can you do???

Cyber SME: What effects do you want?

Unfortunately this scenario has been repeated multiple times at operational-level headquarters, across all Services and in Joint commands.[3]According to one former J5 Chief of Plans,

> It was a struggle . . . to integrate cyber in campaign and operational planning. Classification was always an obstacle, but my ignorance, time constraints, and what I viewed as resistance from what I would now call the cyber teams involved left cyber considerations as things to be integrated after the core elements of the plan had been developed.[4]

The frustrating result is that relatively little progress has been made in many commands regarding the incorporation of cyberspace into operational-level plans. But if carefully analyzed, the previous illustration not only helps identify problems; it also offers insights into possible solutions.

Obstacle #1: Cyberspace Planner Ignorance.

Why the disconnect? To start, today's cyberspace experts generally come from the Signal and Military Intelligence (MI) branches. These key branches provide the critical, fundamental basis for DoD's emerging cyberspace capabilities because of their valuable network, information system, and Signals Intelligence (SIGINT) expertise. However, because these are not combat arms branches, Signal and MI officers usually do not drive mission analysis or create friendly courses of action. This is one of the reasons why many cyberspace planners currently ask, "What effects do you want?" as this question is based on their support branch backgrounds. It is exacerbated when a number of cyberspace planning courses (which are often set up by instructors with Signal and MI backgrounds) also teach their students to ask this same question.

However, to be effective, cyberspace operations must be an integral part of the friendly courses of action. It is inconceivable to envision an infantry or armor officer asking "What effects do you want?" when developing a friendly COA, because they are expected to drive the creation of friendly courses of action, using the commander's mission, guidance, and end state to determine the best way to defeat the adversary by maximizing the capabilities of the combined arms. Cyberspace planners must learn to have this same action-oriented mindset to effectively incorporate cyberspace operations as part of the combined arms fight. The conversation should sound like this:

G5 lead planner: What can you do?

Cyber SME: Let me study your draft mission, intent, and endstate, and as we go through MDMP, I'll suggest ways to integrate cyberspace into the concept of the operation.

G5 lead planner: Great! Come back for our planning session this afternoon.

The Army has taken the right step in this area by designating its new Cyberspace Branch (17-series) as a maneuver branch, but this change in mindset (i.e., driving the creation of the friendly course of action, not waiting to be told how to support it) should be deliberately fostered as the new branch takes shape.

A related obstacle becomes apparent when looking at *Army Field Manual (FM) 3-94, Theater Army, Corps, and Division Operations*. By purposeful design, MI officers are generally assigned to the G2 and the Intelligence warfighting function, while most Signal officers are assigned to the G6 to support the Mission Command warfighting function. Meanwhile, the Integrating Cells of Current Operations, Future Operations, and Plans, which are run by the G3 and the G5, create friendly COAs and plans.[5] Significantly, the Mission Command warfighting function does not provide subject matter experts to the Integrating Cells. As for the Intelligence Warfighting function, although they are standing members of the Integrating Cells, MI officers typically perform intelligence roles and do not actively create friendly COAs and plans. Even in MDMP exercises in professional military education, Signal and MI officers fill the roles of the G6 and G2, not the G3 or G5. However, the perspectives of the G2 and G6 are significantly different from the G3 and G5; transitioning from the former roles to the latter entails a dramatic shift in perspective, mental outlook, and skills. All of this becomes a major obstacle when a cyberspace expert with a Signal or MI background arrives at an operational-level headquarters to assist with planning, as these cyberspace SMEs, previously assigned to the G2 or G6, will generally have had little to no previous planning experience.[6] This is why U.S. Cyber Command J3 Major General Brett Williams stated, "We have a pressing need to develop cyberspace operators who are credible and effective in the J3 (operations) and J5 (strategic plans and policy) within both the Joint Staff and combatant commands."[7]

How can the Army instill a greater understanding of operational planning in the cyberspace community? First, the goal is not to make cyberspace SMEs into career operational planners, or they will spend a disproportionate time away from cyberspace operations and thus fall short of their true purpose and worth to the Army. It is worth noting that the Army does not have specialized career "intelligence planners," "logistics planners," or "infantry planners," instead, the

Army simply places intelligence, logistics, or infantry officers into planning positions as a career broadening opportunity. Therefore, the goal should be to place cyberspace officers into planning positions after training them to actively participate in and drive planning processes. This will allow them to have productive sessions with G5 planners, informing and developing the entire team. To achieve this, a few structural changes may be all that is needed.

First, during MDMP exercises in professional military education, cyberspace officers should be consistently assigned to G3 or G5 roles, not G2 or G6 roles, where they would be required to determine how cyberspace should be used offensively and defensively as an integrated part of friendly COAs. Another potential exercise would be to have cyberspace officers review and analyze a real-world or example operational-level concept of operations, and then have them recommend how cyberspace should be used offensively and defensively as an integrated part of that concept.

Second, at operational-level headquarters such as Corps, ASCCs, JTFs, and CCMDs, resident offensive and defensive cyberspace planners should be assigned as core members of planning teams convened by the directors of current operations, future operations, and plans. The operational headquarters should also assign cyberspace planners to the G3 and G5, instead of the G2 or G6. These steps would ensure that cyberspace officers build the requisite mindset, planning skills, and experience to actively participate in the creation of friendly COAs. In addition, to rapidly boost the incorporation of cyberspace operations into operational-level planning, the Army should attract its best and brightest cyberspace officers by designating operational-level cyberspace planning positions as key developmental billets. The Army Space Operations Branch (Functional Area 40) has adopted similar measures with a high rate of success, with space operations planners earning a strong reputation at operational-level commands for competence and integration.[8]

Third, as the Army builds its new 17-series Cyberspace Branch, it should consider giving preference to the accession of highly qualified combat arms officers. Because combat arms officers drive plans and operations from the lowest level of command, new cyberspace officers from combat arms branches will already possess the desired mindset and skills to actively create friendly COAs. The Army Cyber Institute, among other organizations, is already aware of cyberspace-talented officers who were recently commissioned into combat arms branches because there was no Cyberspace Branch. Providing some preference to accessing these officers into the new Cyberspace Branch, then providing them with appropriate cyberspace training and experience before placing them into planning positions, will help jump-start the Branch's abilities to incorporate cyberspace into operational plans.

Obstacle #2: G5 Planner Ignorance.

While a few G5 planners have been sent to cyberspace training courses, this is not routine; most operational-level G5 planners, Chiefs of Plans, and G5s are ignorant of cyberspace operations and capabilities. This is significant, as cyberspace officers need the leadership and understanding of the G5 and lead planners to fully incorporate cyberspace operations into friendly COAs. In addition, a G5 lead planner never proposes a friendly course of action to the commander without first going through the G5 Chief of Plans and the G5 at a minimum. If none of those key players—the G5 lead planner, the G5 Chief of Plans, or the G5—understand the basic tenets of cyberspace operations, they cannot have an informed, productive conversation with the cyberspace SME or the commander, and cyberspace operations will not become an integral part of the operational plan.[9]

A related problem comes to light if the G5 lead planner has received cyberspace training, but not the G5 lead planner's chain of command. Without some level of training, the G5 Chief of Plans and the G5 will not be able to assess the sufficiency or effectiveness of recommended cyberspace operations in the proposed friendly COA. They will also struggle to articulate or advocate for some of the weightier aspects of cyberspace operations, such as requesting permissions from higher to conduct offensive cyberspace operations. It is difficult to envision a situation where a G5 lead planner would propose a friendly COA to the commander with no oversight or screening from the G5 Chief of Plans or G5, yet that is exactly what happens regarding cyberspace if the G5 lead planner is familiar with cyberspace operations, but his or her G5 chain of command is not.

There are several valid reasons for these issues. Cyberspace is an emerging domain, much like airpower in the 1920s, and we do not have classroom case studies to impart lessons and knowledge. The lack of cyberspace training and education across Army professional military education is another key point. And, there is no formal recommended or prescribed cyberspace training path for non-cyberspace operational planners. This is why in the conversation above, the G5 lead planner repeatedly asks the cyberspace SME, "What can you do?"

How can the Army instill a greater understanding of cyberspace operations in the planning community? First, the goal is not to make G5 planners into cyberspace experts. Rather, the goal is to make operational-level G5 planners and the G5 chain of command knowledgeable enough about cyberspace operations that they can have a productive planning conversation with the cyberspace

SMEs assigned to the command. Therefore, it would be beneficial for non-cyberspace G5 planners who are assigned to an operational-level headquarters to attend the following three cyberspace courses:

1. Army Cyberspace Operations Planning Course (ACOPC)—2 weeks long, conducted by 1st Information Operations Command at Alexandria, VA, and via Mobile Training Teams (MTTs).
2. Joint Advanced Cyberspace Warfighting Course (JACWC)—4 weeks long, conducted by U.S. Cyber Command (USCYBERCOM) at Fort Meade, MD.
3. Joint Cyberspace Operations Planning Course (JCOPC)—2 weeks long, conducted by U.S. Strategic Command (USSTRATCOM) via MTT.

These courses are nontechnical in nature, teach aspects of cyberspace operations and planning, and, in general, do not overlap each other in content. While sending G5 planners to these courses takes time and money, the payoff to the operational-level command will be significant because the command will be able to better leverage the offensive and defensive capabilities of the cyberspace domain as part of the command's plans.

In the same way, G5 Chiefs of Plans and G5s should attend cyberspace training. Although it would be beneficial for these leaders to attend any of the courses listed, the recommended minimum would be the Army Cyberspace Operations Planning Course (ACOPC), as it provides a good overview, especially regarding the authorities to conduct cyberspace operations. In the long term, the Army can grow G5 senior leader expertise in cyberspace operations by assigning talented non-cyberspace planners to broadening assignments at DoD cyberspace organizations—U.S. Cyber Command, its service components, and the National Security Agency (NSA). By placing planners in organizations where their job is to look at the cyberspace problem full-time, the Army will begin to grow cyberspace-savvy officers who will become G5 leaders. These leaders then will be able to ensure the effective incorporation of cyberspace operations into planning, as well as provide valuable cyberspace operations assistance to others across the staff and to the commander.

Finally, the Army must thoroughly incorporate cyberspace training and education into all levels of Army professional military education. Planners come from all Army branches and backgrounds, so they (as well as all Soldiers) should come into their assignment knowing some of the unclassified basics of cyberspace operations, such as:

- Adversaries create malware to exploit inherent vulnerabilities in software (which is why software patches are important).
- A person or organization often will not know that an adversary is "attacking" them in cyberspace until weeks after the event.
- It can take weeks of careful research to determine (i.e., attribute) who breached your organization's network.

Having this basis of knowledge will help jump-start efforts to incorporate cyberspace operations into planning, as well as increase the vigilance and readiness of the force in general.

Obstacle #3: Cyberspace Domain Ignorance.

Another reason why the G5 lead planner keeps asking the cyberspace SME, "What can you do?" springs from a lack of knowledge on what is in the realm of the possible. A JCOPC instructor recently noted,"[Combatant Commands] continue to ask for clarity on what USCYBERCOM capabilities can be brought to bear. . . . What's within the realm of the possible?"[10] This is due to a scarcity of historical operational analysis on the role and effectiveness of cyberspace in military operations.

A wise senior Army leader once said, "Training teaches you what to do; education teaches you how to think." For example, all Army officers and senior noncommissioned officers receive training on MDMP. In contrast, full-time operational planners receive additional education that helps them learn how to think about planning and operational art. Operational planners analyze historical case studies—battles and campaigns—to see examples of operations, such as envelopments, airborne operations, aerial bombardments, and deception. By examining the actors' objectives, centers of gravity, and other factors, they learn why these operations succeeded or failed, while drawing on a vast catalog of open-source, unclassified historical analyses to study military campaigns in depth. Overall, studying military history is a significant tool; historical case studies help planners understand what is in the realm of the possible and give them ideas to help design and create options when confronted with a novel warfighting problem.

In contrast, there are little to no historical, operational analyses on how cyberspace operations have been integrated into military operations, so operational planners have no concrete examples from which to learn. While one reason for this scarcity is because cyberspace operations are relatively new to military operations, another reason is because the few historical examples that

may exist are so highly classified that experts in operational art cannot study or write about them. Although technical after-action reports on selected cyberspace operations supporting military operations have been written, these typically only narrowly assess how well cyberspace did in hitting a target or defending key terrain. This is not sufficient for an operational planner, who needs a more holistic perspective; in other words, given the objectives of the campaign and desired end state, was this target the right one upon which to use cyberspace operations in the first place? Or would the campaign have been more successful if cyberspace operations were used offensively or defensively elsewhere? In planning, there is no substitute for historical analysis; thus operational planners and senior military leaders are hobbled by not being able to read and discuss the few examples of operational-level cyberspace history that do exist.

How can the Army and Joint community overcome this obstacle? One possibility is to leverage the military's institutions of higher learning and planning, such as the Senior Service Colleges (SSC), the School of Advanced Military Studies (SAMS), the School of Advanced Warfighting (SAW), and the Joint Advanced Warfighting School (JAWS). The faculty and students who specialize in operational art could be encouraged to research and write historical, operational analysis papers on how offensive and defensive cyberspace operations have been integrated into military operations or operational maneuver. There also is an opportunity here for partnership—senior leaders could request joint development of these products, with the added benefit of better relationships and understanding between the professional military education community, the Joint or Army command, and Cyberspace commands.[11]

To conduct this type of research, several challenges must be overcome. First, relevant faculty members and students would have to possess or be submitted for Top Secret/Sensitive Compartmented Information (TS/SCI) security clearances, as most information regarding real-world cyberspace operations currently requires that access. Special Access Program and/or Special Technical Operations accesses should not be necessary, as researchers should be focused on the broader operational picture, not the technical details of cyberspace tools and tactics. Second, all organizations concerned in the research—combatant commands, U.S. Cyber Command and its component commands, NSA, etc.—must agree to support the researchers' work. Without the cooperation of these organizations, creating useful analyses will not be possible. Third, to safeguard classified cyberspace capabilities, while enabling a wider dissemination to the operational planning community, cyberspace operational analysis papers would be written at the SECRET level and maintained in a central Army or Joint repository on the Secret Internet Protocol Router Network (SIPRNet). Again, because researchers should be focused on the broader

operational picture, analyses at this level of classification should be possible. If it is not, then a parallel central Army or Joint repository should be maintained at the TS/SCI level on the Joint Worldwide Intelligence Communications System (JWICS) for papers that must be maintained there. The organization responsible for maintaining the repository could come from either the academic community (such as the Army's Combined Arms Center or the Senior Service Colleges) or from the operational community (such as the Joint Staff or U.S. Cyber Command). Regardless, the main objectives are to conduct analyses from an operational art perspective, not a technical cyberspace perspective, and ensure that students, planners, and commanders can access them. While there are probably few historical examples available now, this framework provides a means to capture current and future lessons learned, gives planners and commanders an idea of what is in the realm of the possible, and enables planners to design new ways that cyberspace operations might be used to accomplish the objectives and desired end state of an operational campaign.

Obstacle #4: Commander Ignorance.

Although the conversation that opened this article suggested many challenges, yet another significant challenge lies at the command level. In short, the plan belongs to the commander. This becomes quickly apparent to any planner who has ever proposed a doctrinally worded mission statement or a carefully crafted course of action to a commander, convinced that he or she is proposing the right solution, only to have the commander say, *"Thanks, but that's not what I want. Go back and do this instead."* This is why the military decisionmaking process dictates that the commander approve and/or provide guidance after mission analysis, COA development, COA approval, and concept of operations development. Because in the end, planners do not sign their names to the plan—the commander does.

Therefore, trained and educated cyberspace officers and G5 planners will fall short of the goal of integrating cyberspace operations into operational-level plans; the commander must be educated on cyberspace operations as well. As Major General Brett Williams, the U.S. Cyber Command J3, stated, "Commanders must develop the same capability to direct operations in the cyber domain since mission success increasingly depends on freedom of maneuver in cyberspace."[12] If commanders do not understand cyberspace operations, they will not be able to provide commander's intent or guidance to incorporate cyberspace operations into the plan. They will also not be adequately equipped to discuss or fight for key authorities from higher headquarters. In addition, uneducated commanders, by default, could "run the risk of inappropriately delegating key operational decisions because they…lack an understanding of the domain."[13]

How can the Army better educate its commanders on cyberspace operations? First, the goal is not to make commanders into cyberspace experts. Rather, the goal is to equip commanders with a broad understanding of cyberspace operations, and to provide a good mental framework upon which future experiences can build; knowledge of specific cyberspace tools or accesses is not necessary.[14] In addition, because incorporating cyberspace operations into military operations is a work in progress, and because we seek creative application of cyberspace at the operational level, the long-term goal should be to **educate** Army senior leaders (i.e., how to think), not **train** them (i.e., what to do). Because effective education takes time, discussion, and reflection, one long-term solution is to ensure that Army senior leaders who will become commanders are encouraged to take a semester-long cyberspace elective course while attending a Senior Service College (SSC). While incorporating cyberspace operations into SSC core curriculum is needed, a semester-long elective can much more effectively provide future commanders with the appropriate level of depth and discussion. Officers attending Fellowships or nontraditional SSCs should be likewise encouraged to incorporate cyberspace studies in their programs.[15] Factors such as technology, command and control structures, and authorities will change significantly over the next few years, but even one elective course can provide a sound foundation for future assignments.

Although it is impossible to predict which SSC attendees will become future senior commanders, future commanders will most certainly attend an SSC. In addition, those senior officers who take cyberspace elective courses but do not become commanders will still serve on operational and strategic level staffs, and their greater understanding will certainly facilitate the incorporation of cyberspace operations into military operations and plans. It is important to note that no one knows what the next war will look like, where it will be, or who it will be against, but it will certainly include some aspect of cyberspace operations, whether offensive, defensive, or both. This implies that commanders who have some education in cyberspace operations will have a discernible advantage over commanders who do not, because they will be able to employ their planners and cyberspace SMEs more effectively and thus better leverage the offensive and defensive capabilities of another warfighting domain to augment their operations. It is likely that this will become apparent even in the near future, as Brigade Combat Team (BCT) commanders encounter an extremely capable World Class Cyber Opposing Force (WCCO) at the National Training Center, and it is not unreasonable to expect that BCT commanders with some education in cyberspace will fight more effectively against a cyberspace-wielding adversary than BCT commanders who have little to no education. Therefore, it is in the Army's best interest to

encourage all prospective BCT commanders (some of whom will become the Army's future operational-level commanders) to take a cyberspace operations elective or qualify in a certificate program.

However, one challenge to effectively educating the Army's future operational-level commanders is that only about 15 percent of the U.S. Army War College's annual resident class can take a cyberspace operations elective because of limited capacity. Another challenge is that most of the officers who currently take these electives come from the Signal and MI branches, not the combat arms branches.[16] To resolve these challenges, it would be beneficial if all SSCs expanded their capacity or realigned their electives to allow more students to take a cyberspace operations elective course. The goal could be determined based on analysis of key billets across the force and may be as high as 30 to 40 percent of annual resident class populations; a certificate program could meet some of the demand in this area.[17] In addition, if too many students request enrollment in the cyberspace electives, priority should be given to officers from the combat arms branches. Making these relatively inexpensive changes will go a long way in building Army commanders and senior leaders who can understand, talk about, and effectively leverage cyberspace operations to their advantage, both in operations and planning.

Conclusion.

Overall, successfully incorporating cyberspace operations into operational-level planning involves much more than simply training cyberspace planners. In fact, there are several major systemic obstacles that have hindered the incorporation of cyberspace into operational plans, and addressing this system-wide problem requires a system-wide solution. Admittedly, learning about and trying to incorporate the cyberspace domain into military operations is hard; many capabilities and processes are still being developed, command and control structures continue to evolve, and the Services are experimenting with multiple ideas. However, the ongoing effort to incorporate cyberspace operations into operational-level planning strongly and directly supports the Army's drive to develop mentally agile, adaptive leaders,[18] as leveraging this new domain requires a willingness to learn, an attitude of collaboration, a spirit of creativity, and an ability for leaders to not default back to "what you know." We all have heard the time-worn lament that the Army prepares to fight the last war, not the next war. By taking measures now to successfully incorporate cyberspace operations into operational-level planning, the Army will position itself much more advantageously to fight our next war, for cyberspace operations will be an inescapable, integral part of it.

ENDNOTES

1. *Joint Publication 3-0, Joint Operations,* Washington, DC: Joint Staff, August 11, 2011, p. IV-2.

2. Chief of Staff of the Army Cyberspace Quarterly Update Briefing, Washington, DC, September 2, 2014; and U.S. Air Force Major General Brett T. Williams in "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Forces Quarterly*, 2nd Qtr, 2014, p. 14.

3. This scenario is based on author experience, and confirmed by Navy and Marine Corps cyberspace planners during Cyber Beacon Conference 2014, National Defense University, Washington, DC, July 15-16, 2014. This same lack of understanding is also described in Jason Bender, "The Cyberspace Operations Planner," *Small Wars Journal*, November 5, 2013, available from *smallwarsjournal.com/printpdf/14857*, accessed December 4, 2014.

4. Interview with Colonel Matt Dawson, Director, Center for Strategic Leadership and Development, U.S. Army War College, Carlisle, PA, March 2, 2015.

5. *Army Field Manual (FM) 3-94, Theater Army, Corps, and Division Operations,* Washington, DC: Headquarters, Department of the Army, April 21, 2014, pp. 1-9.

6. There are two possible exceptions: 1) Signal or MI officers who were originally commissioned into combat arms branches, or 2) Signal or MI officers who have extensive experience at the Division level, as Divisions generally operate under a compressed timeframe and draw Signal and MI officers more actively into planning.

7. Williams, p. 14.

8. Interview with Colonel James Meisinger, FA40, HQDA G3/5/7, Washington, DC, February 10, 2015.

9. An operational headquarters once asked U.S. Army Cyber Command (ARCYBER) for assistance in incorporating cyberspace operations into one of its contingency plans. The G5 lead planner told ARCYBER that he was rewriting the concept of operations based on his Commander's updated guidance, but he refused to share the guidance or concept of operations with ARCYBER. He insisted that ARCYBER should be able to write the Cyberspace Appendix without this information, as he incorrectly assumed that cyberspace operations were not related to the friendly scheme of maneuver. Because the G5 chain of command was similarly uninformed about cyberspace operations, ARCYBER's efforts to support the command were delayed by several months.

10. Brett Patron, "Joint Cyberspace Planner Training MTT" briefing, Yorktown, VA, September 19, 2012, available from *www.dtic.mil/doctrine/training/conferences/wjtsc12_2/wjtsc12_2_cti_mtt.pdf*, accessed December 9, 2014.

11. Dawson interview.

12. Williams, p. 12.

13. *Ibid*., pp. 12-13.

14. Bender.

15. In addition, the SSCs could develop cyberspace certificate programs and mandate them as requirements for students not able or willing to take cyberspace electives. This requirement could extend to distance education programs, with a goal of key billets across the force having a cyberspace certificate as a prerequisite for assignment. Dawson interview.

16. Telephonic interview with Professor Bill Waddell, Director, Mission Command and Cyber Division, U.S. Army War College, Carlisle, PA, December 9, 2014.

17. Dawson interview.

18. Army Capabilities Integration Center, ARCIC, "Army Warfighting Challenge #10: 'Develop Agile and Adaptive Leaders'," March 6, 2015, available from *www.arcic.army.mil/app_Documents/ARCIC_AUSA-Flyer_Army-Warfighting-Challenges_06MAR15.pdf*, accessed March 11, 2015.

*****